PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2021

Superintendencia de Industria y Comercio

Enero, 2021

CONTENIDO

NOMBRE DEL DOCUMENTO	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
VIGENCIA	2021	
CREADO POR	Grupo de Trabajo de Informática Forense y Seguridad Digital	Fecha: Enero, 2021
REVISADO POR	Eduar Enrique Navarro Morales Coordinador Grupo de Trabajo de Informática Forense y Seguridad Digital	Fecha: Enero, 2021
APROBADO POR	Francisco Andrés Rodríguez Eraso Jefe Oficina Tecnología e Informática	Fecha: Enero, 2021

CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
1.0	Enero de 2020	Creación del documento
2.0	Enero de 2021	Actualización de documento por cambio de vigencia

1 INTRODUCCION

De acuerdo con lo estipulado en el numeral 2.1.3 del Manual de Gobierno Digital, el plan de seguridad y privacidad de la información establece los detalles de cómo se realizará la implementación y mejora de la seguridad de la información en la Entidad para cada vigencia, estipulando directrices, tiempos y responsables, de tal forma que se logren resultados anuales mejores que en la vigencia anterior.

Es de anotar que, en anteriores vigencias la SIC ha desarrollado proyectos que han permitido acceder, entre otros, a los siguientes beneficios:

- Contar con metodologías para la identificación y clasificación de activos, gestión de riesgos e incidentes de seguridad de la información.
- Contar con políticas de seguridad de la información.
- Fortalecer la conciencia en cuanto a las amenazas y riesgos en el ciberespacio a los que se enfrentan los colaboradores en sus labores diarias.
- Implementación de controles del Sistema de Gestión de Seguridad de la Información – SGSI.
- Establecer un proceso estratégico cuyo objetivo es proteger la información institucional.
- Contar con procedimientos, instructivos y formatos que orientan la gestión del SGSI.
- Identificar riesgos que pueden afectar la seguridad de la información en los procesos de la Entidad.

2 OBJETIVO

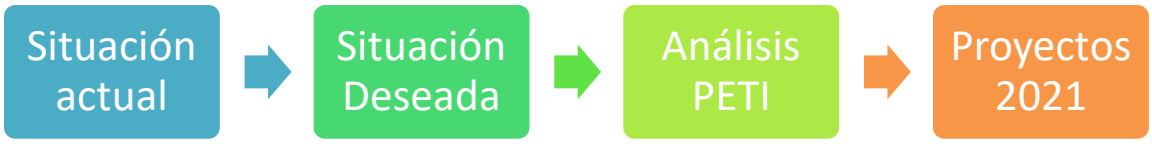
Establecer las acciones estratégicas tendientes a fortalecer la seguridad y privacidad de la información en la Superintendencia de Industria y Comercio - SIC, mediante la planeación de actividades para la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI de la Entidad para la vigencia 2021.

3 ALCANCE

El presente documento se encuentra articulado con el plan de acción institucional para el año 2021, Plan de Tratamiento de Riesgos de Seguridad de la Información y Plan Estratégico de Tecnologías de Información (2019-2022).

4 METODOLOGÍA

Para definir los proyectos del presente plan se analizó la situación actual vs la deseada, buscando en todo momento una alineación con el PETI. El resumen de la metodología se muestra a continuación:



4.1 SITUACIÓN ACTUAL

Respecto a los resultados del MIPG del año 2019, se obtuvo un puntaje de 81.1% para la Política de Seguridad Digital, encontrando que para la vigencia 2021 es necesario la mejora continua en los siguientes dominios de control:

- A.7 Seguridad de los RRHH.
- A.8. Gestión de activos.
- A.10. Controles criptográficos.
- A.14 Adquisición de sistemas, desarrollo y mantenimiento.
- A.16 Gestión de los incidentes de seguridad.
- A.17 Continuidad del negocio.
- A.18 Cumplimiento con requerimientos legales y contractuales.

Lo anterior se sustenta en los resultados de la auditoría interna de seguridad de la información vigencia 2020, en la cual se evidenciaron 9 hallazgos, los cuales se listan a continuación:

- Hallazgo No.1 Debilidades en la Identificación y actualización de requisitos legales y normatividad de Seguridad de la Información.
- Hallazgo No. 2. Debilidades en el tratamiento de riesgos de seguridad de la información y sus controles asociados.
- Hallazgo No. 3. Procedimiento de controles criptográficos no documentado.
- Hallazgo No. 4. Debilidades en la inspección de sistemas de Información.
- Hallazgo No. 5. Debilidades en la medición del cumplimiento de objetivos (indicadores).
- Hallazgo No. 6. Debilidades en la gestión de incidentes de seguridad de la Información.
- Hallazgo No. 7. Debilidades en controles de seguridad de instalaciones físicas y del cableado.

- Hallazgo No. 8. Inobservancia del Manual Operativo de MIPG en el marco del Decreto 1499 de 2017.

Así mismo, en el análisis de brechas del Modelo de Seguridad y Privacidad de la Información – MSPI realizado en diciembre de 2020, se obtuvo el siguiente resultado:

De la gráfica anterior, se identifican aspectos por mejorar en los siguientes controles de seguridad de la información:

ITEM	DESCRIPCIÓN	ISO
Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	A.6.2.1
Etiquetado de la información	Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el	A.8.2.2

ITEM	DESCRIPCIÓN	ISO
	esquema de clasificación de información adoptado por la organización.	
Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	A.9.2.3
Respaldo de la información	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	A.12.3.1
Reglamentación de controles criptográficos.	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	A.18.1.5
Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	A.18.2.3

4.2 SITUACIÓN DESEADA

El SGSI como proceso transversal pretende apoyar el logro de las metas institucionales, aportando desde la perspectiva de seguridad de la información en todos los proyectos en los que se encamine la Entidad.

Como segundo aspecto, procura dar estricto cumplimiento a las políticas y procedimientos de seguridad de la información, bajo un enfoque de sensibilización y concienciación de todas las partes interesadas, destacando el compromiso de la alta dirección con las estrategias de seguridad de la información.

En tercer lugar, espera contar con un esquema robusto de monitoreo y respuesta a incidentes de seguridad de la información que permita responder adecuadamente y minimizar el impacto en la Entidad.

También se deben cerrar las brechas en la implementación de controles, encontradas en la auditoría Interna para superar una eventual auditoría de certificación en la Norma ISO 27001 vigente.

Adicionalmente, es importante implementar controles para proteger la privacidad de la información en todas las dependencias, según el programa integral de protección de datos personales.

También es importante contar con una Entidad preparada ante desastres que puedan afectar el normal funcionamiento, operación y prestación de los servicios al ciudadano.

Finalmente, se busca brindar seguridad en el actual contexto de la Entidad, donde los funcionarios y contratistas en su mayoría se encuentran en la modalidad de trabajo en casa y expuestos a diferentes vectores de ataque.

4.3 ANÁLISIS PETI

Se requiere del SGSI el apoyo en el logro de los objetivos y necesidades de TI, fortaleciendo el cumplimiento de los lineamientos de desarrollo seguro de software en el marco de la metodología DevSecOps, de tal forma que se mitiguen los riesgos de seguridad asociados a su implementación, adicionalmente el análisis y mitigación de riesgos de la información gestionada en tecnologías en la nube.

5 PROYECTOS ESPECIFICOS 2021

Teniendo en cuenta el análisis previo, para la vigencia 2021 se ejecutarán los siguientes proyectos de seguridad de la información.

1. Implementar controles técnicos y de gobierno que fortalezcan la seguridad en entornos de nube pública.
2. Implementar los lineamientos de arquitectura para el desarrollo seguro de software.
3. Fortalecer la gestión de incidentes de seguridad incorporando un enfoque preventivo y aprovechando las capacidades del SOC.
4. Implementar el programa de capacitación y sensibilización en seguridad de la información.
5. Fortalecer controles de seguridad de la información, según el análisis de brechas y la auditoría interna.
6. Apoyar la implementación del Programa Integral de Protección de Datos Personales
7. Implementar las estrategias de recuperación ante Desastres.
8. Apoyar y monitorear la implementación del Plan de Tratamiento de Riesgos de Seguridad de la Información

A continuación, se detalla el alcance de cada proyecto:

Nombre	**Implementar controles técnicos y de gobierno que fortalezcan la seguridad en entornos de nube pública.**
Descripción y contexto	La nube es una tecnología que está ganando un espacio en la SIC por sus ventajas como la escalabilidad, facilidad en la operación, disponibilidad, competitividad, entre otros. No obstante, requiere especial atención desde el campo de la seguridad para definir controles y mitigar riesgos que puedan afectar a la Entidad dado su contexto de exposición frente a ciberamenazas. En ese sentido este proyecto busca, en primer lugar, crear un gobierno, con la definición de políticas, procedimientos, roles y responsabilidades frente a la gestión de la infraestructura e información en la nube y en segundo lugar, implementar herramientas que permitan identificar y corregir brechas de seguridad, así como monitorear posibles fugas de información a través de servicios (Software as a Service) SAAS actualmente contratados o servicios no autorizados por la Entidad.
Recursos OTI	Grupo de Trabajo de Informática Forense y Seguridad Digital Grupo de Trabajo de Servicios Tecnológicos
Áreas involucradas	OTI
Fecha de inicio estimada	1 febrero de 2021
Fecha de fin estimada	30 noviembre 2021

Nombre	**Implementar los lineamientos de arquitectura para el desarrollo seguro de software.**
Descripción y contexto	La Entidad actualizó en el 2020 su metodología de desarrollo de software, pasando de un esquema tradicional a una metodología ágil. En ese sentido, la seguridad debe adaptarse para que los controles definidos se sigan aplicando sin entorpecer el principio de dinamismo de esta nueva metodología. Para lo anterior, en el 2020 se definieron lineamientos de arquitectura para el desarrollo seguro de software, no obstante, algunos no se encuentran implementados.

	En este sentido, este proyecto busca hacer efectivos aquellos lineamientos que actualmente se encuentran en etapa de definición.
Recursos OTI	Grupo de trabajo de sistemas de Información Grupos de trabajo de Gestión de información y proyectos informáticos. Grupo de Trabajo de Servicios Tecnológicos Equipo de arquitectura Empresarial Grupo de Trabajo de Informática Forense y Seguridad Digital
Áreas involucradas	OTI
Fecha de inicio estimada	1 febrero de 2021
Fecha de fin estimada	30 septiembre 2021

Nombre	**Fortalecer la gestión de incidentes de seguridad incorporando un enfoque preventivo y aprovechando las capacidades del SOC.**
Descripción y contexto	Actualmente el Centro de Operaciones de Seguridad - SOC viene desempeñando un rol importante en la detección y respuesta a amenazas cibernéticas, no obstante, se ha evidenciado una falta de articulación con el Grupo de Trabajo de Informática Forense y Seguridad Digital para generar estrategias de prevención y aprendizaje de eventos de seguridad de información. Por lo cual este proyecto busca generar protocolos de manejo de eventos de seguridad, comunicación continua y la implementación de una estrategia preventiva frente a ciberamenazas.
Recursos OTI	Grupo de Trabajo de Informática Forense y Seguridad Digital Grupo de Trabajo de Servicios Tecnológicos
Áreas involucradas	OTI
Fecha de inicio estimada	1 febrero de 2021

Fecha de fin estimada	30 septiembre 2021

Nombre	**Implementar el programa de capacitación y sensibilización en seguridad de la información.**
Descripción	De acuerdo con el Modelo de Seguridad y Privacidad de la Información la capacitación de las personas es un aspecto fundamental para la gestión eficiente de la seguridad de la información, actualmente se ha adelantado campañas de sensibilización, pero no de capacitación. En este sentido, este proyecto busca desarrollar actividades articuladas con el plan institucional de capacitación para fortalecer el conocimiento de colaboradores de la SIC sobre las políticas de seguridad de la información, buenas prácticas, amenazas y controles en un entorno físico y digital.
Recursos OTI	• Grupo de Trabajo de Informática Forense y Seguridad Digital
Áreas involucradas	OTI Oficina de Servicios al Consumidor y de Apoyo Empresarial Grupo de Desarrollo de Talento Humano
Fecha de inicio estimada	1 febrero de 2021
Fecha de fin estimada	30 noviembre 2021

Nombre	**Fortalecer controles de seguridad de la información, según el análisis de brechas y la auditoría interna.**
Descripción	Implementar actividades tendientes a fortalecer los siguientes controles de seguridad: • Política para dispositivos móviles • Etiquetado de la información • Acuerdos de confidencialidad o de no divulgación • Gestión de derechos de acceso privilegiado • Respaldo de la información • Reglamentación de controles criptográficos. • Revisión de cumplimiento técnico.

Recursos OTI	Grupo de Trabajo de Informática Forense y Seguridad Digital Grupo de Trabajo de Servicios Tecnológicos
Áreas involucradas	OTI
Fecha de inicio estimada	1 febrero de 2021
Fecha de fin estimada	30 septiembre 2021

Nombre	**Apoyar la implementación del Programa Integral de Protección de Datos Personales**
Descripción	En el 2020 se definió e implementó un programa integral de protección de datos personales en la SIC, el cual requiere la mejora continua. Este proyecto tiene el objetivo de mejorar la gestión de la privacidad mediante la implementación de una herramienta de control e inventario de las bases de datos que contienen datos personales, así como la revisión independiente del Programa y la subsanación de posibles vulnerabilidades que pueden llegar a exponer datos personales a través de sistemas de información.
Recursos OTI	Grupo de trabajo de Informática Forense y Seguridad Digital.
Áreas involucradas	Secretaria General
Fecha de inicio estimada	1 abril de 2021
Fecha de fin estimada	15 diciembre 2021

Nombre	**Implementar las estrategias de recuperación ante Desastres.**
Descripción	Durante la vigencia 2020 se desarrolló la planificación del DRP, identificando procesos y sistemas de información críticos, tiempos de recuperación, escenarios de riesgo y definiendo estrategias de recuperación. Este proyecto busca darle continuidad a lo trabajado previamente, buscando implementar estrategias de recuperación según la hoja de ruta definida.
Recursos OTI	Grupo de Trabajo de Informática Forense y Seguridad Digital

	Grupo de Trabajo de Servicios Tecnológicos
Áreas involucradas	OTI
Fecha de inicio estimada	1 febrero de 2021
Fecha de fin estimada	30 noviembre 2021

Nombre	**Apoyar y monitorear la implementación el Plan de Tratamiento de Riesgos de Seguridad de la Información**
Descripción	Este proyecto busca darle continuidad a la gestión de riesgos de seguridad de la información, actualmente alineada con la metodología de riesgos institucional, donde la OTI brinda asesoría, acompañamiento y apoyo a las diferentes dependencias de la Entidad en la implementación de las actividades definidas en el plan de tratamiento de riesgos de seguridad de la información. Adicionalmente, en conjunto con la Oficina Asesora de Planeación, analiza los resultados del monitoreo de los riesgos y establece acciones ante las deviaciones en la ejecución del plan.
Recursos OTI	Grupo de Trabajo de Informática Forense y Seguridad Digital
Áreas involucradas	Todas las Dependencias
Fecha de inicio estimada	1 febrero de 2021
Fecha de fin estimada	30 noviembre 2021

_____

Fin documento